doi:10.3969/j.issn.1000-436x.2013.03.010

破解 HFEM 公钥密码方案

古春生[1,2,3]

(1. 江苏理工学院 计算机工程学院，江苏 常州 213001；2. 中国科学技术大学 计算机科学与技术学院，安徽 合肥 230027；
3. 常州市云计算与智能信息处理重点实验室，江苏 常州 213001)

摘 要：为设计后量子公钥密码，赵永哲等人提出了一种基于 BMQ 问题新的公钥方案。利用有限域上遍历矩阵的性质，从该方案公钥能够直接求出其等价私钥，从而破解了该 HFEM 公钥密码方案。

关键词：后量子密码；基于 MQ 的公钥密码；BMQ 问题；密码分析

中图分类号：TP309.2 **文献标识码**：A **文章编号**：1000-436X(2013)03-0085-05

Breaking the HFEM public key scheme

GU Chun-sheng[1,2,3]

(1. School of Computer Engineering, Jiangsu University of hnology, Changzhou 213001, China;
2. School of Computer Science and Technology, University of Science and Technology of China, Hefei 230027, China;
3. Key Laboratory of Cloud Computing & Intelligent Information Processing of Changzhou City, Changzhou 213001, China)

Abstract: To design post-quantum public key cryptography, Zhao, *et al* presented a novel public key scheme based on the BMQ problem. An equivalent secret key could directly be solved from the public key of their scheme by applying the property of the ergodic matrix over finite field. Thus, the HFEM public key scheme was broken.

Key words: post-quantum cryptography; MQ-based PKC; BMQ problem; cryptanalysis

1 引言

由于计算数论上的因式分解问题、离散对数问题和椭圆曲线对数问题存在多项式时间量子算法[1,2]，因此，研究既能抵抗经典密码分析技术，又能抵抗量子密码分析技术的公钥密码方案是公钥密码学发展中的重要问题。目前设计抗量子计算的公钥密码方案成为密码学研究的热点之一。当前密码学界认为能抗量子计算的公钥密码方案主要有基于散列问题的公钥密码、基于编码问题的公钥密码、基于格问题的公钥密码、基于多变量问题的公钥密码等[3]。在这些公钥密码方案中，基于多变量的公钥密码因其计算速度快，密码膨胀率低的特点而成为“后量子密码学”研究的重要方向。近年来，设计构造基于遍历矩阵性质的密码原语已经引起了研究人员的广泛关注[4~9]。文献[4~6,8]研究了 GF(2^k)上的遍历矩阵性质，并给出了其在加密数据、生成伪随机数、生成信息摘要、Shamir 三次传递协议等密码学上的应用，文献[10~12]利用遍历矩阵研究了公钥密码协议的半群作用问题。文献[13]构造了基于有限域上遍历矩阵的双侧幂乘问题的公钥加密方案。文献[14]基于 BMQ 问题(bisection multivariate quadratic equation problem)的困难性提出了隐藏域上遍历矩阵的公钥密码方案。尽管文献[14]证明了有限域上 BMQ 问题是 NP 完全，但并没有证明基于隐藏域上公钥密码方案的安全性。本文主要构造破解文献[14]中 HFEM(hidden field ergodic matrices)公钥密码方案的多项式时间算法。

本文多项式时间破解算法非常简单，即根据文献[14]的方案公钥中隐藏的遍历矩阵性质求出一个

收稿日期：2011-12-14；修回日期：2013-01-31
基金项目：国家自然科学基金资助项目(61142007)；常州市应用基础研究基金资助项目(CJ20120021)；江苏理工学院科研基金资助项目(KYY12027, KYY11055)
Foundation Items: The National Natural Science Foundation of China (6114 07); The Application Research Foundation of Changzhou (CJ20120021); The Research Foundation of Jiangsu University of Technology (KYY12027, KYY11055)

等价私钥，然后利用这个私钥对密文直接解密。具体说即通过分析发现文献[14]的公钥矩阵具有形式 $\boldsymbol{WB}_1, \boldsymbol{WB}_2$，并且 $\boldsymbol{W}$ 可逆，矩阵 $\boldsymbol{B}_1$、$\boldsymbol{B}_2$ 属于同一个遍历矩阵 E 的生成集，即 $\boldsymbol{B}_1 = \boldsymbol{E}^{b_1}$，$\boldsymbol{B}_2 = \boldsymbol{E}^{b_2}$，因而能够计算出矩阵 $\boldsymbol{B}_0 = (\boldsymbol{WB}_1)^{-1} \times \boldsymbol{WB}_2 = \boldsymbol{B}_1^{-1}\boldsymbol{B}_2 = \boldsymbol{E}^{b_2 - b_1}$。根据遍历矩阵性质，矩阵 $\boldsymbol{B}_0$ 属于遍历矩阵 $\boldsymbol{E}$ 的生成集。然后，本文利用 $\boldsymbol{B}_0$ 依次求出 HFEM 公钥密码方案的一个等价私钥。

2 赵永哲等人的 HFEM 公钥密码方案

为完整性，本节自适应地引用文献[14]中相关问题的定义和基于 HFEM 的公钥密码方案。

为叙述方便，本文采用文献[14]中同样符号。设 $\boldsymbol{F}_q^{n\times m}$ 为有限域 F_q 上所有 $n\times m$ 矩阵集，$\boldsymbol{GL}_n(F_q)$ 为有限域 F_q 上非奇异 $n\times n$ 矩阵集，$\boldsymbol{I}$ 为单位矩阵，$\overline{\boldsymbol{M}}$ 为矩阵 $\boldsymbol{M}$ 的元素按行排列后所对应列向量，$\boldsymbol{M}^{-1}$ 为矩阵 $\boldsymbol{M}$ 在有限域 F_q 上的逆矩阵。设 E 为一遍历矩阵生成元，记 $F_q[E] = \{E^k \mid k \in Z\}$。

设矩阵集 $\boldsymbol{A} \subseteq \boldsymbol{F}_q^{n\times m}$，$\boldsymbol{B} \subseteq \boldsymbol{F}_q^{m\times k}$，记 $\boldsymbol{AB} = \{A_iB_j \mid A_i \in \boldsymbol{A} \wedge B_j \in \boldsymbol{B}\} \subseteq \boldsymbol{F}_q^{n\times k}$。设 $x, y \in \boldsymbol{F}_q^n$，记向量张量积 $x \otimes y = (x_1y_1, \text{L}, x_1y_n, \text{L}, x_ny_1, \text{L}, x_ny_n) \in F_q^{n^2}$。

定义 1 BMQ-问题：S 为 F_q 上有 m 个方程和 $2n$ 个变量的方程组，其每个方程形式可表示为

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{i,j}^{(k)} x_i y_j = b_k, (a_{i,j}^{(k)}, b_k \in F_q, k = 1, 2, \text{L}, m)$$

试求方程组 S 的一个解 $(x_1, \text{L}, x_n, y_1, \text{L}, y_n) \in F_q^{2n}$。

定义 2 设矩阵集合 $\boldsymbol{B} = \{B_1, \text{L}, B_k\} \subseteq \boldsymbol{F}_q^{n\times m}$ 线性无关，记 $V_S(\boldsymbol{B}) = \{\sum_{i=1}^{k} x_i \boldsymbol{B}_i \mid x_i \in F_q\}$，称为由集合 $\boldsymbol{B}$ 所生成的 k 维矩阵空间。

为易于证明，笔者自适应地引用文献[14]中基于 HFEM 的公钥密码方案如下。

密钥生成如下。

1) 随机选择矩阵集 $(\boldsymbol{A}, \boldsymbol{B})$。这里 $\boldsymbol{A} = \{A_1, \text{L}, A_n\} \subset \boldsymbol{F}_q^{2\times n}$，$\boldsymbol{B} = \{B_1, \text{L}, B_n\} \subset \boldsymbol{F}_q^{n\times n}$，要求满足 $\boldsymbol{A}$ 线性无关，且 $\boldsymbol{B}$ 是遍历矩阵 $\boldsymbol{E}$ 生成矩阵集 $F_q[\boldsymbol{E}]$ 的基；

2) 随机选择变换矩阵 $\boldsymbol{R} \in \boldsymbol{GL}_{2n}(F_q)$，并计算 $\boldsymbol{R}_{\boldsymbol{AB}} = R[\overline{\boldsymbol{AB}}] \in \boldsymbol{F}_q^{2n\times n^2}$；

3) 由 $R_{\boldsymbol{AB}}$ 生成 $2n$ 个 BMQ 多项式 $[r_1(x,y), \text{L}, r_{2n}(x,y)]^{\text{T}} = R_{\boldsymbol{AB}} \times (x \otimes y)^{\text{T}}$；

4) 公钥为 $pk = (F_q, r = [r_1(x,y), \text{L}, r_{2n}(x,y)])$，私钥为 $sk = (\boldsymbol{A}, \boldsymbol{B}, R)$。

加密算法如下。

1) 明文消息为 $P = a \otimes b$ $(a, b \in F_q^n \setminus \{0\})$；

2) 给定公钥 pk 和明文 P，计算输出密文 $C = [r_1(a,b), \text{L}, r_{2n}(a,b)] \in F_q^{2n} \setminus \{0\}$。

解密算法如下。

1) 给定私钥 sk 和密文 C，计算 $T = (R^{-1} \times C) \in (V_S(\boldsymbol{A})V_S(\boldsymbol{B})) \setminus \{0\}$；

2) 给定私钥 sk 和 T，解出方程组 $E(\boldsymbol{A}, \boldsymbol{B}, T)$ 的一组非零解：$(x,y) \in (F_q^n \setminus \{0\})^2$；

3) 根据 (x,y) 与 (a,b) 等价，计算输出明文 $P = x \otimes y = a \otimes b$。

根据文献[14]，方程组 $E(\boldsymbol{A}, \boldsymbol{B}, T)$ 定义为：$\left[\overline{\boldsymbol{AB}}\right].(x \otimes y)^{\text{T}} = \overline{T}$，这里 $\text{Rank}(\left[\overline{\boldsymbol{AB}}\right]) = 2n$。定义 $\left[\overline{\boldsymbol{AB}}\right] = \left[\overline{A_1B_1}, \text{L}, \overline{A_1B_n}, \text{L}, \overline{A_nB_1}, \text{L}, \overline{A_nB_n}\right]$，注意等式左边符号 $\left[\overline{\boldsymbol{AB}}\right]$ 系符号混用，仅表示矩阵符号，目的是与文献[14]中原文一致，并不表示矩阵 $\boldsymbol{A}, \boldsymbol{B}$ 相乘后再将 $\boldsymbol{AB}$ 的元素按行排列后所对应列向量。在已知 $(\boldsymbol{A}, \boldsymbol{B})$ 的情况下，方程组 $E(\boldsymbol{A}, \boldsymbol{B}, T)$ 易于求解。

3 破解 HFEM 公钥密码方案

尽管文献[14]证明了 BMQ 问题是 NP 难的(定理 1)，但文献[14]并没有归约 HFEM 公钥密码方案的安全性到求解 BMQ 问题。通过分析上述 HFEM 公钥密码方案，笔者知道破解公钥方案的关键是求出 $V_S(B)$ 的一个基。为此，首先给出与遍历矩阵相关的 2 个引理。

引理 1 假定 $f(l)$ 为遍历矩阵 $\boldsymbol{E}$ 的特征多项式。如果 $|F_q[\boldsymbol{E}]| = q^n - 1$，则 $f(l)$ 为次数为 n 的不可约多项式。

证明 因 $f(l) = |l\boldsymbol{I} - \boldsymbol{E}|$，故 $f(l)$ 为次数为 n 的多项式。用反证法，假定 $f(l)$ 是可约的，则 $f(l)$ 或者是不可约多项式的幂，或者可以表示成 2 个互素多项式的积。下面分别证明它们是矛盾的。

1) $f(l)$ 可表示成 2 个互素多项式的乘积。

不失一般性，设 $f(l) = g_1(l)g_2(l)$，$\deg(g_1(l)) = k$，$1 \le k < n$，$\deg(g_2(l)) = n - k$ 和 $\gcd(g_1(l),$

$g_2(l))=1$。

因 $\boldsymbol{E}$ 为遍历矩阵，故 $f(0)=|\boldsymbol{E}|\neq 0$，所以 $g_1(0)\neq 0, g_2(0)\neq 0$。

由 $\deg(g_1(l))=k$ 和 $g_1(0)\neq 0$，可知剩余类环 $F_q[l]/(g_1)$ 只包含 q^k-1 个非零元素，所以剩余类集合 $\{l^i \mid i=0,\L,q^k-1\}$ 中存在 2 个非零元素 l^r, l^s 满足 $l^r\equiv l^s \bmod g_1(l)$，即存在正整数 $0<e_1\leq q^k-1$ 满足 $l^{e_1}\equiv 1 \bmod g_1(l)$。

同理可证存在正整数 $0<e_2\leq q^{n-k}-1$，满足 $l^{e_2}\equiv 1 \bmod g_2(l)$。

由 $\gcd(g_1(l), g_2(l))=1$，得 $l^{e_1e_2}\equiv 1 \bmod f(l)$，并且 $0<e_1e_2<q^n-1$。

因 $|F_q[\boldsymbol{E}]|=q^n-1$ 和 $f(l)$ 为遍历矩阵 $\boldsymbol{E}$ 的特征多项式，故满足 $l^e\equiv 1 \bmod f(l)$ 的最小正整数是 $e=q^n-1$。

所以 $(q^n-1)\mid(e_1e_2)$，矛盾。

2) $f(l)$ 是不可约多项式的幂，即 $f(l)=g(l)^r$, $r\geq 2$。因 $g(l)$ 为不可约多项式，且 $g(0)\neq 0$，则 $e=q^{n/r}-1$ 是满足 $l^e\equiv 1 \bmod g(l)$ 的最小正整数。故 $f(l)=g(l)^r \mid (l^{q^{n/r}-1}-1)^r$。

因 F_q 为有限域，故 F_q 中元素个数一定是某个素数的幂。设素数 p 是 F_q 的特征，则 F_q 有 p^k 个元素，这里 k 是 F_q 在素域 F_p 的扩张次数。设 v 是满足 $p^v\geq r$ 的最小正整数。因为 $(l^{q^{n/r}-1}-1)^r \mid (l^{q^{n/r}-1}-1)^{p^v}=l^{p^v(q^{n/r}-1)}-1$，则 $l^{p^v(q^{n/r}-1)}\equiv 1 \bmod f(l)$。

又因 $e=q^n-1$ 是满足 $l^e\equiv 1 \bmod f(l)$ 的最小正整数，所以 $(q^n-1)\mid(p^v(q^{n/r}-1))$。因 $l\geq 2$，矛盾。

根据遍历矩阵特征多项式的不可约性可以得到有限域 F_q 上模 $f(l)$ 的多项式 $F_q[l]$ 产生多项式的有限域，与遍历矩阵同构。

引理 2　假定 $\boldsymbol{E}$ 为遍历矩阵且 $|F_q[\boldsymbol{E}]|=q^n-1$，$f(l)$ 为 $\boldsymbol{E}$ 的特征多项式，则矩阵集 $\boldsymbol{B}=\{E^0, E^1, \L, E^{n-1}\}$ 为遍历矩阵集 $F_q[\boldsymbol{E}]$ 的基。

证明　由引理 1 知，$f(l)$ 为次数 n 的不可约多项式，因此，剩余类环 $F_q[l]/(f)$ 中任意元素对应次数小于 n 的多项式 $r(l)$，即 $\left|F_q[l]/(f)\right|=q^n$。又因 $\boldsymbol{E}^k$ 与有限域 F_q 上次数小于 n 的 $r(l)=l^k \bmod f(l)$ 一一对应，即在有限域 F_q 上矩阵 $\boldsymbol{E}^k$ 等于 $r(\boldsymbol{E})$。而 $r(\boldsymbol{E})$ 中所有 $\boldsymbol{E}$ 的次数小于 n，即 $F_q[\boldsymbol{E}]$ 中任意元素可以用 $\boldsymbol{B}$ 表示。同理可以证明，由 $\boldsymbol{B}$ 生成的元素也属于 $F_q[\boldsymbol{E}]\cup\{0\}$。

因 $f(l)$ 为 $\boldsymbol{E}$ 的不可约特征多项式，故 $f(\boldsymbol{E})$ 为关于矩阵 $\boldsymbol{E}$ 满足 $g(\boldsymbol{E})=0$ 的多项式中最小次数的多项式。故矩阵集 $\boldsymbol{B}$ 线性无关。因此，$\boldsymbol{B}$ 是 $F_q[\boldsymbol{E}]$ 的基。

定理 1　假定 $\boldsymbol{B}=\{E^{b_1}, E^{b_2}, \L, E^{b_n}\}$ 是 $F_q[\boldsymbol{E}]$ 的一个基，则 $\boldsymbol{B}'=\{\boldsymbol{I}, E^{b_2-b_1}, \L, E^{b_n-b_1}\}$ 也是 $F_q[\boldsymbol{E}]$ 的一个基。

证明　如果 $\boldsymbol{B}'$ 线性无关，则 $\left|V_S(\boldsymbol{B}')\right|=q^n$，即 $V_S(\boldsymbol{B}')=F_q[\boldsymbol{E}]\cup\{0\}$。反证法，假定 $\boldsymbol{B}'$ 线性相关，则存在一组非全 0 数 $k_i\in F_q(i=1,\L,n)$ 满足 $k_1\boldsymbol{I}+k_2E^{b_2-b_1}+\L+k_nE^{b_n-b_1}=0$。因为 $E^{b_1}\neq 0$，故 $E^{b_1}(k_1\boldsymbol{I}+k_2E^{b_2-b_1}+\L+k_nE^{b_n-b_1})=E^{b_1}\times 0$，即 $k_1E^{b_1}+k_2E^{b_2}+\L+k_nE^{b_n}=0$。因此 $\boldsymbol{B}$ 线性相关，矛盾。

定理 2　假定 $\boldsymbol{B}=\{B_1,\L,B_n\}\subset \boldsymbol{F}_q^{n\times n}$、$\boldsymbol{A}=\{A_1,\L,A_n\}\subset \boldsymbol{F}_q^{2\times n}$ 和 $R\in \boldsymbol{GL}_{2n}(F_q)$。给定公钥 $R_{\boldsymbol{AB}}=R[\overline{\boldsymbol{AB}}]\in \boldsymbol{F}_q^{2n\times n^2}$，则存在多项式时间算法求解 $F_q[\boldsymbol{E}]$ 的一个基 $\boldsymbol{B}'=\{\boldsymbol{I}, B_1^{-1}B_2, \L, B_1^{-1}B_n\}$。

证明　为了根据密码方案的公钥 $R_{\boldsymbol{AB}}$ 求解 $F_q[\boldsymbol{E}]$ 的一个基，首先将 HFEM 公钥密码方案中公钥写成下面矩阵形式。

$$
\begin{aligned}
R_{\boldsymbol{AB}} &= R[\overline{\boldsymbol{AB}}] \\
&= \boldsymbol{R}^{2n\times 2n}\times\begin{pmatrix}A_1\\A_2\\ \M \\A_n\end{pmatrix}^{2n\times n}\times\begin{pmatrix}B_1 & B_2 & \L & B_n\end{pmatrix}^{n\times n^2} \\
&= \begin{pmatrix}R_{11}^{n\times n} & R_{12}^{n\times n}\\ R_{21}^{n\times n} & R_{22}^{n\times n}\end{pmatrix}\times\begin{pmatrix}Q_1^{n\times n}\\ Q_2^{n\times n}\end{pmatrix}\times\begin{pmatrix}B_1 & B_2 & \L & B_n\end{pmatrix}^{n\times n^2} \\
&= \begin{pmatrix}R_{11}Q_1+R_{12}Q_2\\ R_{21}Q_1+R_{22}Q_2\end{pmatrix}^{2n\times n}\times\begin{pmatrix}B_1 & B_2 & \L & B_n\end{pmatrix}^{n\times n^2} \\
&= \begin{pmatrix}W_1B_1 & W_1B_2 & \L & W_1B_n\\ W_2B_1 & W_2B_2 & \L & W_2B_n\end{pmatrix}^{2n\times n^2}
\end{aligned}
$$

其中，$\boldsymbol{R}^{2n\times 2n}=\begin{pmatrix}R_{11}^{n\times n} & R_{12}^{n\times n}\\ R_{21}^{n\times n} & R_{22}^{n\times n}\end{pmatrix}$，$\boldsymbol{A}^{2n\times n}=\begin{pmatrix}Q_1^{n\times n}\\ Q_2^{n\times n}\end{pmatrix}$，$\boldsymbol{RA}=\begin{pmatrix}W_1^{n\times n}\\ W_2^{n\times n}\end{pmatrix}=\begin{pmatrix}R_{11}Q_1+R_{12}Q_2\\ R_{21}Q_1+R_{22}Q_2\end{pmatrix}$。

因为 $R\in \boldsymbol{GL}_{2n}(F_q)$，$\boldsymbol{A}$ 线性无关，由文献[15]

可知：

$\mathrm{rank}(\boldsymbol{R})+\mathrm{rank}(\boldsymbol{A})-2n \le \mathrm{rank}(\boldsymbol{RA}) \le \min(\mathrm{rank}(\boldsymbol{R}), \mathrm{rank}(\boldsymbol{A}))$。

因此，$\mathrm{rank}(\boldsymbol{RA})=n$。不失一般性，设 $W_1 \in \boldsymbol{GL}_n(F_q)$，即在有限域 F_q 上 W_1 可逆。

又因为 $B_1 \in \boldsymbol{GL}_n(F_q)$，知 W_1B_1 可逆。故可以计算 $B_2^{'}=(W_1B_1)^{-1}\times W_1B_2=B_1^{-1}B_2$ 和 $Q_1^{'}=W_1B_1$。因此，可以计算得到 $\boldsymbol{B}'=\{\boldsymbol{I}, B_1^{-1}B_2, \cdots, B_1^{-1}B_n\}$ 和 $\boldsymbol{A}'=\begin{pmatrix} W_1B_1 \\ W_2B_1 \end{pmatrix}$。根据定理 1 可知 $\boldsymbol{B}'$ 是 $F_q[\boldsymbol{E}]$ 的基。

显然，易于证明上述求解 $\boldsymbol{B}', \boldsymbol{A}'$ 算法所需时间是多项式时间算法。因为使用高斯消元法计算 $\boldsymbol{B}_1$ 的逆矩阵 $\boldsymbol{B}_1^{-1}$ 需要时间为 $O(n^3)$；计算 $\boldsymbol{B}'$ 中矩阵乘积 $\boldsymbol{B}_1^{-1}\ \boldsymbol{B}_i$，$i$=2,…, n 需要时间为 $(n-1)\times O(n^3)=O(n^4)$；计算 $\boldsymbol{A}'$ 需要时间为 $2\times O(n^3)=O(n^3)$。这里假定 F_q 上任意一次算术运算需要时间为 1 个单位时间。

定理 3 给定公钥 $R_{\boldsymbol{AB}}=R[\overrightarrow{\boldsymbol{AB}}] \in \boldsymbol{F}_q^{2n\times n^2}$ 和密文 $C \in \boldsymbol{F}_q^{2\times n} \setminus \{0\}$，则存在多项式时间算法恢复密文中的明文。

证明 根据定理 2，可以在多项式时间内求解 $\boldsymbol{B}', \boldsymbol{A}'$，且 $\boldsymbol{B}'$ 也是 $F_q[\boldsymbol{E}]$ 的基。

1) 根据文献[14]HFEM 公钥密码方案，设 $C=ab=\left(\sum_{i=1}^{n} x_i A_i^{'}\right)\left(\sum_{j=1}^{n} y_j B_j^{'}\right)$。

2) 由遍历矩阵性质，知 $\left(\sum_{j=1}^{n} y_j B_j^{'}\right)^{-1}$ 存在，令 $b^{-1}=\sum_{j=1}^{n} z_j B_j^{'}$，则可得联立方程组：

$$E(x,z): \left(\sum_{i=1}^{n} x_i A_i^{'}\right)=\left(\sum_{j=1}^{n} z_j (CB_j^{'})\right)。$$

3) 求解该方程组 $E(x,z)$ 得一组非零解 $(x,z) \in (F_q^n \setminus \{0\})^2$。

4) 由 $(\boldsymbol{B}', z)$ 求出 $b^{-1}=\sum_{j=1}^{n} z_j \boldsymbol{B}_j^{'}$，再用高斯消元法求逆得 b。

5) 计算 b 在基 $\boldsymbol{B}'$ 下满足 $b=\sum_{j=1}^{n} y_j \boldsymbol{B}_j^{'}$ 的向量 $y \in \boldsymbol{F}_q^n \setminus \{0\}$。则 (x,y) 为 $E(\boldsymbol{A}', \boldsymbol{B}', C)$ 的一个解。

6) 由 (x,y) 求出 $E(\boldsymbol{A}', \boldsymbol{B}', C)$ 的全部 $(q-1)$ 个相互等价的解：$\{(dx, d^{-1}y) \mid d \in F_q \setminus \{0\}\}$。

7) 根据 HFEM 公钥密码方案，计算输出明文 $P=x \otimes y$。

4 破解 HFEM 公钥密码方案举例(n=3，q=5)

本节通过实例演示破解 HFEM 公钥算法。首先生成 HFEM 公钥；然后根据公钥求解基 $\boldsymbol{B}'$ 和 $\boldsymbol{A}'$；最后根据 HFEM 公钥密码方案对密文进行解密。

4.1 生成 HFEM 公钥

设遍历矩阵 $\boldsymbol{E}=\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$，$\boldsymbol{B}=\{\boldsymbol{I}, \boldsymbol{E}^{55}, \boldsymbol{E}^{110}\}=\left\{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 1 & 2 \\ 1 & 1 & 2 \\ 3 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 4 & 1 \\ 3 & 0 & 4 \end{pmatrix}\right\}$。

随机选择矩阵 $\boldsymbol{A}=\begin{Bmatrix} A_1 \\ A_2 \\ A_3 \end{Bmatrix}=\left\{\begin{pmatrix} 3 & 3 & 2 \\ 4 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 2 \\ 4 & 3 & 4 \end{pmatrix}\right\}$，

$$\boldsymbol{R}=\begin{pmatrix} 2 & 3 & 0 & 1 & 4 & 3 \\ 1 & 4 & 4 & 2 & 2 & 1 \\ 0 & 2 & 3 & 1 & 1 & 0 \\ 2 & 3 & 1 & 4 & 0 & 0 \\ 2 & 1 & 1 & 4 & 1 & 0 \\ 1 & 1 & 2 & 2 & 1 & 1 \end{pmatrix}。$$

根据定理 1 可知，选择 $\boldsymbol{B}$ 只要为 $F_q[\boldsymbol{E}]$ 的基即可，易于验证上述选择的 $\boldsymbol{B}$ 符合条件。计算输出公钥为

$$R_{\boldsymbol{AB}}=R\left[\overrightarrow{\boldsymbol{AB}}\right]=\boldsymbol{RAB}=\boldsymbol{R}\times\begin{pmatrix} A_1B_1 & A_1B_2 & A_1B_3 \\ A_2B_1 & A_2B_2 & A_2B_3 \\ A_3B_1 & A_3B_2 & A_3B_3 \end{pmatrix}$$

$$=\begin{pmatrix} 4 & 3 & 1 & 3 & 3 & 0 & 2 & 1 & 2 \\ 0 & 2 & 3 & 1 & 0 & 2 & 4 & 3 & 4 \\ 4 & 4 & 3 & 0 & 1 & 4 & 3 & 0 & 1 \\ 3 & 2 & 1 & 4 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 4 & 0 & 0 & 1 & 3 & 1 & 1 \\ 2 & 2 & 1 & 1 & 0 & 4 & 0 & 0 & 1 \end{pmatrix}。$$

4.2 求解基 $\boldsymbol{B}'$ 和 $\boldsymbol{A}'$

现根据定理 2，使用公钥 $R_{\boldsymbol{AB}}$ 计算 $F_q[\boldsymbol{E}]$ 的基 $\boldsymbol{B}'$ 和 $\boldsymbol{A}'$ 如下。

1) 首先重写 $R_{\boldsymbol{AB}}=\begin{pmatrix} W_1B_1 & W_1B_2 & W_1B_3 \\ W_2B_1 & W_2B_2 & W_2B_3 \end{pmatrix}=$

$$\left(\begin{pmatrix}4&3&1\\0&2&3\\4&4&3\end{pmatrix}\ \begin{pmatrix}3&3&0\\1&0&2\\0&1&4\end{pmatrix}\ \begin{pmatrix}2&1&2\\4&3&4\\3&0&1\end{pmatrix}\right.$$
$$\left.\begin{pmatrix}3&2&1\\1&0&4\\2&2&1\end{pmatrix}\ \begin{pmatrix}4&1&1\\0&0&1\\1&0&4\end{pmatrix}\ \begin{pmatrix}1&1&1\\3&1&1\\0&0&1\end{pmatrix}\right);$$

2)计算 W_1B_3 逆

$$(W_1B_3)^{-1}=B_3^{-1}W_1^{-1}=\begin{pmatrix}2&1&2\\4&3&4\\3&0&1\end{pmatrix}^{-1}=\begin{pmatrix}3&4&3\\3&1&0\\1&3&2\end{pmatrix}$$

3) 计算 $\boldsymbol{B}_1'=B_3^{-1}W_1^{-1}W_1B_1=B_3^{-1}B_1=\begin{pmatrix}4&4&4\\2&1&1\\2&2&1\end{pmatrix}$，

$\boldsymbol{B}_2'=\begin{pmatrix}3&2&0\\0&4&2\\1&0&4\end{pmatrix}$，$\boldsymbol{B}_3'=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$；

4) 计算 $\boldsymbol{W}_1=\begin{pmatrix}2&1&2\\4&3&4\\3&0&1\end{pmatrix}$，$\boldsymbol{W}_2=\begin{pmatrix}1&1&1\\3&1&1\\0&0&1\end{pmatrix}$；

5) 设 $\boldsymbol{A}_1'=\begin{pmatrix}2&1&2\\4&3&4\end{pmatrix}$，$\boldsymbol{A}_2'=\begin{pmatrix}3&0&1\\1&1&1\end{pmatrix}$，

$\boldsymbol{A}_3'=\begin{pmatrix}3&1&1\\0&0&1\end{pmatrix}$。

4.3 加密算法

给定公钥 R_{AB}，设明文为 $P=a\otimes b=(4\quad 2\quad 3)\otimes(2\quad 3\quad 1)$。计算密文如下

$$C=[r_1(a,b),\cdots,r_{2n}(a,b)]=R\left[\overline{\boldsymbol{AB}}\right]P^{\mathrm{T}}$$
$$=\sum_{i=1}^{3}\sum_{j=1}^{3}(a_ib_j)A_i'B_j'=\begin{pmatrix}3&4&0\\2&1&1\end{pmatrix}$$

4.4 解密算法

1) 根据文献[14]和求解的基 $\boldsymbol{B}'$ 和 $\boldsymbol{A}'$ 可列方程组 $E(\boldsymbol{A}',\boldsymbol{B}',C)$

$$C=ab=(\sum_{i=1}^{3}x_iA_i')(\sum_{j=1}^{3}y_jB_j')$$

2) 设 $b^{-1}=\sum_{j=1}^{n}z_jB_j'$。则可得联立方程组

$$E(x,z)：\left(\sum_{i=1}^{n}x_iA_i'\right)=\left(\sum_{j=1}^{n}z_j(CB_j')\right)$$

3) 求解该方程组 $E(x,z)$ 得一组非零解 $x=(3\quad 4\quad 1)$，$z=(1\quad 0\quad 2)$。

4) 由 $(\boldsymbol{B}',z)$ 求出 $b^{-1}=\sum_{j=1}^{n}z_jB_j'=\begin{pmatrix}1&4&4\\2&3&1\\2&2&3\end{pmatrix}$，

再用高斯消元法求逆得 $b=\begin{pmatrix}4&2&4\\2&0&4\\1&2&0\end{pmatrix}$。

5) 计算 b 在基 $\boldsymbol{B}'$ 下满足 $b=\sum_{j=1}^{n}y_jB_j'$ 的向量 $y=(1\quad 4\quad 3)$。则 (x,y) 为 $E(\boldsymbol{A}',\boldsymbol{B}',C)$ 的一个解。由 (x,y) 易于求出 $E(\boldsymbol{A}',\boldsymbol{B}',C)$ 相互等价的 $(q-1)$ 个解：$\{(dx,d^{-1}y)\mid d\in F_q\setminus\{0\}\}$。

6) 输出明文 $P'=x\otimes y$。易于验证明文 $P=P'$。

5 结束语

利用遍历矩阵的性质，本文给出从 HFEM 公钥密码方案的公钥直接求解其等价私钥的多项式时间算法，从而破解了文献[14]设计的 HFEM 公钥密码方案。最后，通过计算示例演示 HFEM 公钥密码方案的破解过程。

参考文献：

[1] SHOR P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(5):1484-1509.

[2] PROOS J, ZALKA C. Shor's discrete logarithm quantum algorithm for elliptic curves[J]. Quantum Information and Computation, 2003, 3(4):317-344.

[3] BUCHMANN J, DING J T. Post-quantum cryptography[A]. The Second International Workshop, PQCrypto 2008[C]. Cincinnati, USA, 17-19.

[4] 赵永哲，黄声烈，姜占华. GF(2^k)上的遍历矩阵及其特性分析[J]. 小型微型计算机系统, 2005, 26 (12):2135-2139.
ZHAO Y Z, HUANG S L, JIANG Z H. Ergodic matrix over GF (2^k) and its properties[J]. Mini-micro Systems, 2005, 26 (12):2135-2139.

[5] ZHAO Y Z, WANG L O, ZHANG W. Information-exchange using the ergodic matrices in GF(2)[A]. 2nd International Conference, ACNS 2004[C]. Amsterdam: Icisa Press, 2004. 388-397.

[6] 赵永哲，裴士辉，王洪军等. 利用有限域上的遍历矩阵构造动态加密器[J]. 小型微型计算机系统, 2007, 28 (11): 2010-2014.
ZHAO Y Z, PEI S H, WANG H J, *et al*. Using the ergodic matrices over finite field to construct the dynamic encryptor[J]. Mini-Micro Systems, 2007, 28 (11):2010-2014.

[7] PEI S H, ZHAO H W, ZHAO Y Z. Public key cryptography based on ergodic matrices over finite field[J]. Wuhan University Journal of Natural Sciences, 2006, 11(6):1525-1528.

[8] 赵永哲，姜占华，黄声烈. 基于 F_2 上遍历矩阵的 Shamir 三次传递协议的实现[J]. 小型微型计算机系统, 2006, 27(6):986-991.
ZHAO Y Z, JIANG Z H, HUANG S L. Implementation of Shamir's three pass protocol based on ergodic matrix over finite field[J]. Mini-Micro Systems, 2006, 27(6):986-991.

（下转第 98 页）

[13] 3G Americas, MIMO and smart antennas for 3G and 4G wireless systems: practical aspects and deployment considerations[EB/OL]. http://www.4gamericas.org/, 2010.

[14] EDELMAN A. Eigenvalues and Condition Number of Random Matrices[D]. Dept Mathematics, MIT, Cambridge, MA, 1989.

[15] OESTGES C, CLERCKX B. MIMO Wireless Communications: From Real-World Propagation to Space-Time Code Design[M]. Burlington: Academic Press, 2007.

[16] TSE D, VISWANATH P. Fundamentals of Wireless Communication[M]. Cambridge, UK: Cambridge University Press, 2005.

[17] TULINO A M, VERDU S. Random Matrix Theory and Wireless Communications[M]. Boston: Now Publishers Inc, 2004.

[18] KYOSTI P, MEINILA J, HEBTUKA L. WINNER II channel mode : part II radio channel measurement and analysis results[EB/OL]. http://www.ist-winner.org/, 2007.

作者简介：

罗万团（1981-），男，广西南宁人，西南交通大学博士生，主要研究方向为高铁环境下的群切换、多天线分集技术、MIMO 系统设计和应用。

方旭明（1962-），男，浙江义乌人，博士，西南交通大学教授、博士生导师，主要研究方向为无线宽带接入控制、无线资源管理、多跳中继网络、高铁宽带无线接入。

程梦（1986-），女，湖北武汉人，西南交通大学博士生，主要研究方向为高铁环境下的协作分集、智能多天线技术。

周祥娟（1986-），女，四川广安人，硕士，南京中兴新软件有限责任公司操作系统及支撑软件开发助理工程师，主要研究方向为高铁环境下多点协作传输、切换技术。

（上接第 89 页）

[9] **孙永雄，赵永哲，杨永健等. 基于遍历矩阵的单向(陷门)函数的构造方案**[J]. **吉林大学学报: 信息科学版**, 2006, 24(5):555-560.
SUN Y X, ZHAO Y Z, YANG Y J, *et al*. Scheme to construct one-way (trapdoor) functions based on ergodic matrices[J]. Journal of Jilin University: Information Science Edition, 2006, 24(5):555-560.

[10] MONICO C. Semirings and Semigroup Actions in Public-Key Cryptography[D]. Notre Dame: University of Notre Dame, 2002.

[11] MAZE G. Algebraic Methods for Constructing One-Way Trapdoor Functions[D]. Notre Dame: University of Notre Dame, 2003.

[12] **黄华伟.半群作用问题在密码学中的应用**[D]. **西安: 西安电子科技大学**, 2008.
HUANG H W. Cryptographic Applications of Semigroup Action Problem[D]. Xi'an: Xidian University, 2008.

[13] **裴士辉,赵永哲,赵宏伟. 基于遍历矩阵的公钥加密方案**[J]. **电子学报**, 2010, 38(8):1908-1913.
PEI S H, ZHAO Y Z, ZHAO H W. Public key encryption scheme based on the ergodic matrices[J]. Chinese Journal of Electronics, 2010, 38(8):1908-1913.

[14] **赵永哲,赵博,裴士辉等**. HFEM **公钥密码方案的设计与实现**[J]. **通信学报**,2011,32(6):24-31.
ZHAO Y Z, ZHAO B, PEI S H, *et al*. Design and implement on the HFEM public key scheme[J]. Journal on Communications, 2011,32(6): 24-31.

[15] HORN R A, JOHNSON C R. Matrix Analysis[M]. Cambridge University Press, 2005.

作者简介：

古春生（1971-），男，安徽芜湖人，博士，江苏理工学院副教授，主要研究方向为公钥密码学。